Most of the existing security monitoring solutions cannot cope with unknown and complex attacks due to the continual apparition of new threats, botnet propagation and command-and-control mechanisms. Recently, botnet detection systems which leverage communication graph analysis using machine learning have gained attention to overcome these limitations. Graph-based modeling and mining approaches have been proposed and provide interesting results.

Graph-based modeling offers the advantage of understanding complex attacks and determining the root cause of an attack. However, existing graph mining tools for anomaly detection over streaming events are not adapted for cyber-security problems while the corresponding data continuously appears in the form of complex graphs.

The workshop serves to bring together people from industry and academia including researchers, developers, and practitioners from a variety of fields working on graphs and their applications to network, cybersecurity, and blockchain. Moreover, the workshop allows attendees to share and discuss their latest findings from both theoretical and practical perspectives in several techniques and methods for graph modeling, mining, learning, and visualizing. The main goal of GraSec is to present research and experience results in graph applications on network and cybersecurity as well as the defensive and offensive tools.

TPC CO-CHAIRS

- Sofiane Lagraa (SnT, University of Luxembourg)
- Radu State (SnT, University of Luxembourg)
- Hamida Seba (LIRIS, University of Lyon, France)
- Martin Husák (Masaryk University, Czech Republic)

PROCEEDINGS

Papers accepted for GraSec 2020 will be included in the conference proceedings, IEEE Xplore, IFIP database and EI Index. IFIP and IEEE reserve the right to remove any paper from the IFIP database and IEEE Xplore if the paper is not presented at the workshop.

IMPORTANT DATES

- Paper Submission Deadline: **January 8th, 2021**
- Notification of Acceptance: **February 18th, 2021**
- Submission of Camera-ready Copies: **March 5th, 2021**

WEB

- https://grasec.uni.lu

CONTACT US

- Sofiane Lagraa: sofiane.lagraa[@]uni.lu
- Martin Husák: husakm[@]ics.muni.cz

TOPICS OF INTEREST

Authors are invited to submit papers that fall into or are related to one or multiple topic areas listed below:

- Graph modeling/mining/learning-based intrusion/botnet/threats detection
- Graph learning-driven access controls, security policies, etc.
- Attack graphs modeling, analysis, etc.
- Sampling and summarizing techniques of graphs for network and cyber-security.
- Big graph analytics, parallel algorithms for dynamic/big graph analysis on HPC (CPU-GPU) systems.
- Autoencoders, representation learning for graphs
- Graph embedding techniques and applications on network data.
- Visualization of dynamic and large-scale graphs
- Detection of threats with evolving behaviors using graphs
- Novel applications of static/dynamic and large graph problems in network, cybersecurity, blockchain, cryptocurrency, robot, etc.

PAPER SUBMISSION

Paper submissions must present original, unpublished research, development or experiences. Only original papers that have not been published or submitted for publication elsewhere can be submitted. Each submission must be written in English, accompanied by a 50 to 200 words abstract that clearly outlines the scope and contributions of the paper. Self-plagiarized papers will be rejected without further review. Authors should submit their papers via JEMS: https://jems.sbc.org.br/

LIKELY CONTRIBUTORS

Contributors should attempt to submit relevant contributions on a topic, including cross-disciplinary work. However, there types of contributors are expected: 1. Theoretical and empirical papers. 2. Position papers. 3. Reproducible papers.

PAPER FORMAT

There is a length limitation of **6 pages** (including title, abstract, all figures, tables, and references) for **regular papers**, and **4 pages** for **short papers** describing work in progress. Submissions must be in **IEEE 2-column** style.

ACCEPTED PAPER

The **accepted regular papers**, they will have a 20 minutes oral presentation (including Q&A) at assigned time slot. The **accepted short papers**, they will have a 5 minutes oral presentation (excluding Q&A) and a poster presentation at assigned time slot. The size of the poster is recommendation to be Ao (33.1 × 46.8 in) or smaller.